## Basic information

| | |
|---|---|
| **2005/0182(COD)**<br><br>COD - Ordinary legislative procedure (ex-codecision procedure)<br>Directive | Procedure completed |
| Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes<br><br>Amending Directive 2002/58/EC 2000/0189(COD)<br><br>**Subject**<br><br>1.20.09 Protection of privacy and data protection<br>3.30.05 Electronic and mobile communications, personal communications<br>7.30.20 Action to combat terrorism | |

## Key players

### European Parliament

| Committee responsible | Rapporteur | Appointed |
|---|---|---|
| LIBE Civil Liberties, Justice and Home Affairs | PICKART ALVARO Alexander Nuno (ALDE) | 26/09/2005 |

| Committee for opinion | Rapporteur for opinion | Appointed |
|---|---|---|
| ITRE Industry, Research and Energy | NIEBLER Angelika (PPE-DE) | 05/10/2005 |
| IMCO Internal Market and Consumer Protection | CEDERSCHIÖLD Charlotte (PPE-DE) | 24/10/2005 |

### Council of the European Union

| Council configuration | Meetings | Date |
|---|---|---|
| Justice and Home Affairs (JHA) | 2709 | 2006-02-21 |
| Justice and Home Affairs (JHA) | 2696 | 2005-12-01 |

### European Commission

| Commission DG | Commissioner |
|---|---|
| Justice and Consumers | |

## Key events

| Date | Event | Reference | Summary |
|---|---|---|---|
| | | COM(2005)0438 | Summary |

| | | | |
|---|---|---|---|
| 21/09/2005 | Legislative proposal published | | |
| 15/11/2005 | Committee referral announced in Parliament, 1st reading | | |
| 24/11/2005 | Vote in committee, 1st reading | | Summary |
| 28/11/2005 | Committee report tabled for plenary, 1st reading | A6-0365/2005 | |
| 01/12/2005 | Debate in Council | | Summary |
| 13/12/2005 | Debate in Parliament | | |
| 14/12/2005 | Decision by Parliament, 1st reading | T6-0512/2005 | Summary |
| 14/12/2005 | Results of vote in Parliament | | |
| 21/02/2006 | Act adopted by Council after Parliament's 1st reading | | Summary |
| 15/03/2006 | Final act signed | | |
| 15/03/2006 | End of procedure in Parliament | | |
| 13/04/2006 | Final act published in Official Journal | | |

## Technical information

| | |
|---|---|
| **Procedure reference** | 2005/0182(COD) |
| **Procedure type** | COD - Ordinary legislative procedure (ex-codecision procedure) |
| **Procedure subtype** | Legislation |
| **Legislative instrument** | Directive |
| **Amendments and repeals** | Amending Directive 2002/58/EC 2000/0189(COD) |
| **Legal basis** | EC Treaty (after Amsterdam) EC 095 |
| **Stage reached in procedure** | Procedure completed |
| **Committee dossier** | LIBE/6/30671 |

## Documentation gateway

**European Parliament**

| Document type | Committee | Reference | Date | Summary |
|---|---|---|---|---|
| Amendments tabled in committee | | PE364.849 | 27/10/2005 | |
| Amendments tabled in committee | | PE364.972 | 17/11/2005 | |
| Committee opinion | ITRE | PE364.724 | 23/11/2005 | |
| Committee report tabled for plenary, 1st reading/single reading | | A6-0365/2005 | 28/11/2005 | |
| Text adopted by Parliament, 1st reading/single reading | | T6-0512/2005 | 14/12/2005 | Summary |

**European Commission**

| Document type | Reference | Date | Summary |
|---|---|---|---|
| | COM(2005)0438 | | |

| | | | |
|---|---|---|---|
| Legislative proposal | | 21/09/2005 | Summary |
| Document attached to the procedure | SEC(2005)1131 | 21/09/2005 | |
| Commission response to text adopted in plenary | SP(2006)0053 | 12/01/2006 | |
| Follow-up document | COM(2011)0225 | 18/04/2011 | Summary |

**National parliaments**

| Document type | Parliament /Chamber | Reference | Date | Summary |
|---|---|---|---|---|
| Contribution | SE_PARLIAMENT | COM(2011)0225 | 25/11/2011 | |
| Contribution | PT_PARLIAMENT | COM(2011)0225 | 25/02/2012 | |

**Other institutions and bodies**

| Institution/body | Document type | Reference | Date | Summary |
|---|---|---|---|---|
| OS | For information | N6-0029/2005<br>OJ C 298 29.11.2005, p. 0001-0012 | 26/09/2005 | |
| EESC | Economic and Social Committee: opinion, report | CES0035/2006<br>OJ C 069 21.03.2006, p. 0016-0021 | 19/01/2006 | |
| EDPS | Document attached to the procedure | N7-0088/2011<br>OJ C 279 23.09.2011, p. 0001 | 31/05/2011 | Summary |

**Additional information**

| Source | Document | Date |
|---|---|---|
| European Commission | EUR-Lex | |

**Final act**

Directive 2006/0024
OJ L 105 13.04.2006, p. 0054-0063 Summary

# Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 15/03/2006 - Final act

PURPOSE : to harmonise Member States' provisions concerning the obligations of providers of publicly available electronic communications services with respect to the retention of certain data.

LEGISLATIVE ACT : Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

CONTENT : the Council adopted this Directive with the Irish and Slovak delegations voted against. The Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The Directive applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It does not apply to the content of electronic communications, including information consulted using an electronic communications network.

The following categories of data must retained with regard to fixed network telephony and mobile telephony, as well as Internet access, Internet e-mail and Internet telephony:

- data necessary to trace and identify the source of a communication;

- data necessary to trace and identify the destination of a communication;

- data necessary to identify the date, time and duration of a communication;

- data necessary to identify the type of communication;

- data necessary to identify the communication device;

- data necessary to identify the location of mobile communication equipment.

The types of data to be retained under these categories of data are specified in the Directive. With regard to an "unsuccessful call attempt", this is defined as a communication where a telephone call has been successfully connected but is unanswered or there has been a network management intervention. This will include the retention of data in relation to unsuccessful call attempts where that data is generated or processed, and stored (as regards telephony data) or logged (as regards Internet data) by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communication services concerned. The Directive shall not require the retention of data in relation to unconnected calls. Data on an unsuccessful call attempt only has to be retained if the company already stores such data.

No data revealing the content of the communication may be retained pursuant to this Directive.

Member States must ensure that the categories of data specified are retained for periods of not less than six months and not more than two years from the date of the communication. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken and state the grounds for introducing them. The Commission shall, within a period of six months after the notification, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within this period the national measures shall be deemed to have been approved.

The Directive goes on to make provision for data protection and data security. Each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, certain prescribed data security principles with respect to data retained in accordance with the Directive. Each Member State must designate a supervisory authority to be responsible for monitoring the application within its territory of the provisions adopted by the Member States regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC. The supervisory authority must act with complete independence.

No later than 15 September 2010, the Commission must submit an evaluation of the application of the Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data and the periods of retention.

TRANSPOSITION : 15 September 2007. Until 15 March 2009, each Member State may postpone application of the Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this provision must notify the Council and the Commission to that effect by way of a declaration. The following Member States have made such a declaration postponing application for differing lengths of time: the Netherlands, Austria, the United Kingdom, Estonia, Cyprus, Greece, Luxembourg, Slovenia, Sweden, Lithunia, Latvia, Czech Republic, Belgium, Poland, Finland, Germany.

ENTRY INTO FORCE : 03/05/2006.

# Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 21/02/2006

The Council adopted a Directive of the European Parliament and of the Council on data retention,

amending Directive 2002/58/EC. The decision follows an agreement reached by the Council at its meeting on 1 and 2 December 2005.

The Irish and Slovak delegations voted against.

To recall, this Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Following entry into force of the Directive, Member States will have as a general rule 18 months in which to comply with its provisions.

# Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 21/09/2005 - Legislative proposal

PURPOSE : to harmonise provisions concerning processing and retention of data regarding publicly available electronic communications services or public communications for the purpose of preventing and investigating serious criminal offences, and amending Directive 2002/58/EC

PROPOSED ACT : Directive of the European Parliament and of the Council.

CONTENT : Citizens increasingly perform daily activities using electronic communications networks and services. These communications generate 'traffic data' or 'location data' which include details about the location of the caller, the number called, the time and duration of the call. When combined with data

enabling the identification of the user of the service, the availability of such traffic data is important for purposes related to law enforcement. However, with changes in service offerings, such as the growth of flat rate tariffs, pre-paid and free electronic communications services, traffic data may not always be stored by all operators to the same extent as they were in recent years, depending on the services they offer. This trend is reinforced by recent offerings of Voice over IP communication services, or even flat rate services for fixed telephone communications. Under such arrangements, the operators would no longer have the need to store traffic data for billing purposes. If traffic data are not stored for billing or other business purposes, they will not be available for public authorities whenever there is a legitimate case to access the data. These developments are making it much harder for public authorities to fulfil their duties in preventing and combating organised crime and terrorism.

It has now become urgent to adopt harmonised provisions at EU level on this subject. A certain number of Member States have adopted national measures requiring some or all operators to retain given types of data so that they can be used for the purposes identified above when necessary. Differences in the legal, regulatory, and technical provisions in Member States concerning the retention of traffic data present obstacles to the Internal Market for electronic communications as service providers are faced with different requirements regarding the types of data to be retained.

This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a public communications network with respect to the processing and retention of certain data, in order to ensure that the data is available for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime. The Directive applies to traffic and location data of both private and legal persons, as well as the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network. The following categories of data must retained:

-data necessary to trace and identify the source of a communication;

-data necessary to trace and identify the destination of a communication;

-data necessary to identify the date, time and duration of a communication;

-data necessary to identify the type of communication;

-data necessary to identify the communication device;

-data necessary to identify the location of mobile communication equipment.

The types of data to be retained under these categories of data are specified in the Annex.

These categories of data must be retained for a period of one year from the date of the communication, with the exception of data related to electronic communications taking place using wholly or mainly the Internet Protocol. The latter shall be retained for a period of six months.

Statistics on the retention of data must be provided to the European Commission on a yearly basis. Such statistics shall not contain personal data.

Lastly, the Directive must be evaluated three years after transposition.

# Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 31/05/2011 - Document attached to the procedure

**Opinion of the European Data Protection Supervisor on the Evaluation report from the**

**Commission to the Council and the European Parliament on the Directive 2006/24/EC (Data Retention Directive).**

The EDPS recalls that on 18 April 2011, the Commission presented its evaluation report on the Data Retention Directive, and sent the report to the EDPS on the same day. The Data Retention Directive constituted an EU response to urgent security challenges, following the major terrorist attacks in Madrid in 2004 and in London in 2005. Despite the legitimate purpose for setting up a data retention scheme, criticism was voiced in relation to the huge impact the measure had on the privacy of citizens. The EDPS considers that importance of the Evaluation report and the evaluation process cannot be overstated. The Data Retention Directive constitutes a prominent example of an EU measure aiming at ensuring availability of data generated and processed in the context of electronic communications for law enforcement activities. Now that the measure has been in place for several years, an evaluation of its practical application should actually demonstrate the necessity and proportionality of the measure in light of the rights to privacy and data protection. In this respect the EDPS has called the evaluation 'the moment of truth' for the Data Retention Directive.

The EDPS believes that the evaluation procedure should be used to set the standard for the evaluation of other EU instruments regulating information management, including the processing of huge amounts of personal data, in the area of freedom, security and justice. It should ensure that only those measures that are truly justified stay in place.

The EDPS analyses the content of the Evaluation report from a privacy and data protection point of view, focusing on whether the current Data Retention Directive meets the requirements set out by these two fundamental rights. This includes an analysis of whether the necessity of data retention as regulated in the Directive has sufficiently been demonstrated. The report sets out the main content of the Data Retention Directive, and its relationship with Directive 2002/58/EC ('the ePrivacy Directive'), the changes brought about by the Lisbon Treaty, and an analysis on the validity of the Data Retention Directive in light of the rights to privacy and data protection.

**Directive does not meet requirements:** the evaluation report shows that the Directive has failed to meet its main purpose, namely to harmonise national legislation concerning data retention. Such a lack of harmonisation is detrimental to all parties involved: citizens, business operators, as well as law enforcement authorities.

The EDPS' analysis states that the Data Retention Directive does not meet the requirements set out by the rights to privacy and data protection, for the following reasons:

- the necessity of data retention as provided for in the Data Retention Directive has not been sufficiently demonstrated;
- data retention could have been regulated in a less privacy-intrusive way;
- -the Data Retention Directive lacks foreseeability.

It is therefore clear that the Data Retention Directive cannot continue to exist in its present form. In that respect, the Commission rightly proposes a revision of the current data retention framework. .

**Necessity:** the EDPS states that the Commission should have insisted that Member States provide sufficient evidence that demonstrates the necessity of the measure since political statements by some Member States on the need for such a measure cannot alone justify EU action. Before proposing a revised version of the Directive, the EDPS feels that:

- the Commission should, during the impact assessment, invest in collecting further practical evidence from the Member States in order to demonstrate the necessity of data retention as a measure under EU law;
- if a majority of Member States considers data retention to be necessary, these Member States should all provide the Commission with quantitative and qualitative evidence demonstrating it;
- Member States that oppose such a measure of data retention should provide the Commission with information to enable a broader assessment of the matter.

The EDPS underlines that an assessment of the necessity and the examination of alternative, less privacy-intrusive means can only be conducted in a fair way if all options for the future of the Directive are left open. In that respect, the Commission seems to exclude the possibility of repealing the Directive, either per se or combined with a proposal for an alternative, more targeted EU measure. The EDPS therefore calls upon the Commission to seriously consider these options in the impact assessment as well. Only if there is agreement on the need for EU rules from the perspective of the internal market and police and judicial cooperation in criminal matters and if, during the impact assessment, the necessity of data retention, supported and regulated by the EU, can be sufficiently demonstrated, which includes a careful consideration of alternative measures, a future Data Retention Directive can be considered.

The EDPS does not disagree that a well-defined obligation to retain telecommunications data may be justified under certain very strict conditions.

**E-Privacy Directive:** Article 15(1) of the ePrivacy Directive enables Member States to adopt legislative measures to restrict the scope of their obligations regarding the confidentiality of communications and data retention, and it has been used by several Member States. The EDPS has referred to this as a 'legal loophole' in the legal framework, which hampers the purpose of the Data Retention Directive, namely to create a level-playing field for industry.

**Data retention goes beyond what is necessary**: the Evaluation report does permit the conclusion that the Data Retention Directive has regulated data retention in a way which goes beyond what is necessary, or, at least, has not ensured that data retention has not been applied in such a way. The EDPS highlights four elements:

- the unclear purpose of the measure and the wide notion of 'competent national authorities' has led to the use of retained data for far too wide a range of purposes and by far too many authorities, and there is no consistency in the safeguards and conditions for access to the data;
- the maximum retention period of two years appears to go beyond what is necessary, and the lack of a fixed single retention period for all Member States has created a variety of diverging national laws which may trigger complications, because it is not always evident what national law is applicable;
- the level of security is not sufficiently, and a broader consultation and more concrete investigation into instances of abuse is needed;
- it is not clear from the report whether all categories of retained data have proven to be necessary. Only some general distinctions are made between telephone and Internet data.

**Basic requirements for future instrument**: any future EU instrument on data retention should therefore meet the following basic requirements:

- it should be comprehensive and genuinely harmonise rules on the obligation to retain data, as well as on the access and further use of the data by competent authorities;
- it should be exhaustive, which means that it has a clear and precise purpose and that the legal loophole which exists with Article 15(1) of the ePrivacy Directive is closed;
- it should be proportionate and not go beyond what is necessary.

# Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 18/04/2011 - Follow-up document

The Commission presents its evaluation report on Directive 2006/24/EC (the Data Retention Directive). The Directive requires Member States to oblige providers of publicly available electronic communications services or of public communications networks ('operators') to retain traffic and location data for between six months and two years for the purpose of the investigation, detection and prosecution of serious crime.

The report evaluates the application of the directive by Member States and its impact on economic operators and consumers. It aims to determine whether it is necessary to amend the provisions of the Directive, in particular with regard to its data coverage and retention periods. The report also examines the implications of the Directive for fundamental rights, in view of the criticisms which have been levelled in general at data retention, and examines whether measures are needed to address concerns associated with the use of anonymous SIM cards for criminal purposes.

The report highlights a number of benefits of and areas for improvement in the current data retention regime in the EU. The EU adopted the Directive at a time of heightened alert of imminent terrorist attacks. The Commission intends to conduct an **impact assessment** that will provide an opportunity to assess the data retention in the EU against the tests of necessity and proportionality, with regard to and in the interests of internal security, the smooth functioning of the internal market and reinforcing respect for privacy and the fundamental right to protection of personal data. The Commission's proposal for revising the data retention framework should build on its conclusions and recommendations.

**The EU should support and regulate data retention as a security measure**: most Member States take the view that EU rules on data retention remain necessary as a tool for law enforcement, the protection of victims and the criminal justice systems. The evidence, in the form of statistics and examples, provided by Member States is limited in some respects but nevertheless attests to the very important role of retained data for criminal investigation. These data provide valuable leads and evidence in the prevention and prosecution of crime. Their use has resulted in convictions for criminal offences which, without data retention, might never have been solved. It has also resulted in acquittals of innocent persons. Harmonised rules in this area should ensure that data retention is an effective tool in combating crime, that industry has legal certainty in a smoothly functioning internal market, and that the high levels of respect for privacy and the protection of personal data are applied consistently throughout the EU.

**Transposition has been uneven**: transposed legislation is in force in 22 Member States. The considerable leeway left to Member States to adopt data retention measures under the e-Privacy Directive (Directive 2002/58/EC) renders assessment of the Data Retention Directive highly problematic. There are considerable differences between transposed legislation in the areas of purpose limitation, access to data, periods of retention, data protection and data security and statistics. Three Member States (Czech Republic, Germany and Romania) have been in breach of the Directive since their transposing legislation was annulled by their respective constitutional courts. Two further Member States (Austria and Sweden) have yet to transpose. The Commission will continue to work with all Member States to help ensure effective implementation of the Directive. It will also continue in its role of enforcing EU law, ultimately using infringement proceedings if required.

**The Directive has not fully harmonised the approach to data retention and has not created a level-playing field for operators**: the Directive does not in itself guarantee that retained data are being stored, retrieved and used in full compliance with the right to privacy and protection of personal data. The responsibility for ensuring these rights are upheld lies with Member States. The Directive only sought partial harmonisation of approaches to data retention; therefore it is unsurprising that there is no common approach, whether in terms of specific provisions of the Directive, such as purpose limitation or retention periods, or in terms of aspects outside scope, such as cost reimbursement. However, beyond the degree of variation explicitly provided for by the Directive, differences in national application of data retention have presented considerable difficulties for operators.

**Operators should be consistently reimbursed for the costs they incur**: there continues to be a lack of legal certainty for industry. The obligation to retain and retrieve data represents a substantial cost to operators, especially smaller operators, and operators are affected and reimbursed to different degrees in some Member States compared with others, although there is no evidence that telecommunications sector overall has been adversely affected as a result of the Directive. The Commission will consider ways of providing consistent reimbursement for operators.

**Ensuring proportionality in the end-to-end process of storage, retrieval and use**: the Commission will ensure that any future data retention proposal respects the principle of proportionality and is appropriate for attaining the objective of combating serious crime and terrorism and does not go beyond what is necessary to achieve it. It will recognise that any exemptions or limitations in relation to the protection of personal data should only apply insofar as they are necessary. It will assess thoroughly the implications for the effectiveness and efficiency of the criminal justice system and of law enforcement, for privacy and for costs to public administration and operators, of more stringent regulation of storage, access to and use of traffic data. The following areas will be examined in the impact assessment:

- consistency in limitation of the purpose of data retention and types of crime for which retained data may be accessed and used;
- more harmonisation of, and possibly shortening, the periods of mandatory data retention;
- ensuring independent supervision of requests for access and of the overall data retention and access regime applied in all Member States;
- limiting the authorities authorised to access the data;
- reducing the data categories to be retained;
- guidance on technical and organisational security measures for access to data including handover procedures;
- guidance on use of data including the prevention of data mining; and
- developing feasible metrics and reporting procedures to facilitate comparisons of application and evaluation of a future instrument.

The Commission will also consider whether and if so how an EU approach to data preservation might complement data retention.

With reference to the fundamental rights 'check-list' and the approach to information management in the area of freedom, security and justice, the Commission will consider each of these areas according to the principles of proportionality and the requirement of foreseeability. It will also ensure consistency with the ongoing review of the EU data protection framework.

**Next steps**: the Commission will propose a revision of the current data retention framework, and devise a number of options in consultation with law enforcement, the judiciary, industry and consumer groups, data protection authorities and civil society organisations. It will research further public perceptions of data retention and its impact on behaviour. These findings will feed into an impact assessment of the policy options identified which will provide the basis for the Commission's proposal.

# Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 01/12/2005

The Council agreed to reach a "first reading deal" with the European Parliament on a Directive on data retention by the end of the year in spite of reservations made by Ireland, Slovakia and Slovenia.

Some of the elements agreed are as follows :

- serious criminal offences : a reference to serious crime is included in the text of the Directive, as defined by each Member State in its national law. Member States shall have due regard to the crimes listed in Article 2(2) of the Framework Decision on the European Arrest Warrant (2002/534/JHA) and crime involving telecommunications;

- retention periods : Member States should ensure that the categories of data referred to in the draft Directive are retained for periods of not less than 6 months and for a maximum of two years from the date of the communication.

- Internet data : the Council is in favour of an obligation to retain data on Internet access, Internet e-mail and Internet telephony;

- unsuccessful calls : the Council is in favour of including the retention of data in relation to unsuccessful call attempts where that data is generated or processed, and stored (as regards telephony data) or logged (as regards Internet data) by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communication services concerned. This Directive shall not require the retention of data in relation to unconnected calls;

- flexibility : Article 15(1) of Directive 2002/58/EC would continue to apply in relation to data, including data related to unsuccessful calls, which are not specifically required to be retained under the present Directive and therefore fall outside the scope of this Directive, and for retention for purposes, including judicial purposes, other than that covered by this Directive.

# Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 14/12/2005 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted a resolution on data retention by 378 votes in favour, 197 against and 30 abstentions. The final text negotiated beforehand with the Council aims to facilitate judicial co-operation in criminal matters by approximating Member States' legislation on the retention of data processed by telecommunications companies.The amendments finally adopted were a compromise between the PES and EPP groups with the Council and differed in some key points to the draft directive adopted initially by the Civil Liberties Committee. (Please see the document dated 24/11/2005.) The GUE, Greens and UEN groups and some members from the ALDE group voted against the directive in the final vote.  Alexander Nuno **ALVARO** (ALDE, DE) was unhappy with the result of the compromise adopted and withdrew his name as rapporteur.

The main amendments are as follows:

-**Purpose:** the aim is to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The Commission had included the objective of “prevention” which was deleted by Parliament. Members felt that the concept of prevention is too vague and could lead to abuse of the system from national authorities. Parliament also deleted the words “serious criminal offences such as terrorism and organised crime” preferring to use the term “serious crimes”.

**-Period:**The directive will provide for data to be retained by the telecommunications companies for a minimum of 6 months and a maximum of 24 from the date of communication. The Commission had proposed the period of one year

**-Unsuccessful calls:** An "unsuccessful call attempt" is defined as a communication where a telephone call has been successfully connected but is unanswered or there has been a network management intervention. This will include the retention of data in relation to unsuccessful call attempts where that data is generated or processed, and stored (as regards telephony data) or logged (as regards Internet data) by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communication services concerned. The Directive shall not require the retention of data in relation to unconnected calls. Data on an unsuccessful call attempt only has to be retained if the company already stores such data. In a recital, Parliament stated that, “considering that the obligations on providers of electronic communications services should be proportionate, the Directive requires that they only retain such data which are generated or processed in the process of supplying their communications services; to the extent that such data is not generated or processed by those providers, there can be no obligation to retain it. This Directive is not intended to harmonise the technology for retaining data, the choice of which will be a matter to be resolved at national level.”

**Reimbursement of costs:** Parliament decided to delete the paragraph in which it was mandatory for Member States to reimburse telecom companies for all additional costs of retention, storage and transmission of data. In the draft directive adopted by the Civil Liberties Committee, Members had initially called for the full reimbursement of costs.

**-Content:** A new clause is inserted stating that no data revealing the content of the communication can be retained pursuant to this Directive.

**-Type of data:** Parliament tightened up the provisions on types of data to be retained, in Article 4. This includes the registration of location data on calls, SMS and internet use.

**-Supervisory authority:** There is a new clause on supervisory authority. Each Member State must designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States regarding the security of the stored data. These authorities must act with complete independence in exercising their functions.

**-Data protection and data security:** A new clause states that each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, certain prescribed data security principles with respect to data retained in accordance with the Directive.

**-Push system:**Member States must ensure that data retained in accordance with the Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation.

**-Sanctions:** Unauthorised access or transfer of data will be punished by “effective, proportionate or dissuasive” penalties, either administrative or criminal.

**-Future measures:** A new clause has been introduced permitting derogation from the time period. A Member State facing particular circumstances warranting an extension for a limited period of the maximum retention period may take the necessary measures. The Member State shall immediately notify the Commission and inform the other Member States of the measures and indicate the grounds for introducing them. The Commission shall, within six months after the notification, approve or reject the national measures involved after having verified whether or not they are a means of arbitrary discrimination or disguised restriction of trade between Member States and whether or not they shall constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within this period the national measures shall be deemed to have been approved.